GREENBOOK

PROJECTWISE SECURITY

ProjectWise Integration Server
Seguridad

- **Derechos de Acceso**
- **Redes**

www.Bentley.com
communities.Bentley.com

Bentley
Sustaining Infrastructure

Primera Edición (Mayo 2010)
Aplica a:
ProjectWise V8 XM Edition 8.09.xx.xx
ProjectWise V8i Edition 8.11.xx.xx

Aviso Legal: La siguiente información contiene extractos, datos, ejemplos de aplicaciones, instalaciones y configuraciones que se consideran precisas al momento de la publicación. Bentley Professional Services está constantemente actualizando los detalles técnicos, que son sujetos a revisiones. Bentley Professional Services se esfuerza en presentar la información en forma precisa, pero no garantiza su integridad o validez.

El material provisto en esta guía es sólo de consulta, y su utilización es completamente voluntaria. Bentley Professional Services no da garantías, expresas o implícitas, en conexión con esta información. Todo uso o aplicación de esta información es a riesgo y responsabilidad del usuario. Bentley no será responsable por ninguna pérdida, reclamos o daños y perjuicios derivados del uso o aplicación de esta información.

Nota del documento en Español: Este documento es una traducción no-oficial del documento de Bentley Systems Inc.: GreenBook – ProjectWise Systems Architecture. Se ha intentado realizar una traducción completa sin modificar, quitar ni agregar datos. Para descargar el original en inglés de este documento, por favor dirigirse al siguiente link: http://communities.bentley.com/products/projectwise/content_management/w/wiki/5448.aspx

Tabla de Contenidos

Tabla de Contenidos 3

1.0 Introducción a GREENBOOK 5

2.0 Acerca del/los Autor(es) 6

3.0 Resumen del Documento 7

4.0 Conceptos de Permisos de Accesos de ProjectWise 8

4.1 Seguridad del Objeto 14

4.2 Seguridad de Flujo de Trabajo 16

4.3 Autenticación y Encriptado 33

Preguntas Frecuentes sobre Autenticación y Encriptado de ProjectWise 34

¿Qué tipo de encriptado se utiliza cuando un usuario se loguea a la interface Web sin utilizar SSL? 34

¿Qué tipo de encriptado se utiliza cuando un usuario se loguea a la interface Web utilizando SSL? 34

¿Qué tipo de encriptado se utiliza cuando un usuario se loguea a un datasource en ProjectWise Explorer utilizando una cuenta de dominio de Windows? 35

¿Qué tipo de encriptado se utiliza cuando un usuario se loguea a un datasource de ProjectWise Explorer utilizando una cuenta lógica de ProjectWise? 35

¿Qué tipo de encriptado se utiliza cuando un usuario se logue utilizando SSL en el ProjectWise Application Server donde están publicados los datasources (Ejecutando ProjectWise en modo seguro) ? 35

¿Puedo habilitar SSL con ProjectWise Explorer? ¿Se debe modificar la configuración de los puertos? 35

¿Se encripta el archivo cuando se transfiere por el cable utilizando ProjectWise? 35

¿Qué tipo de comunicación segura se realiza cuando se comunica con la base de datos? 35

¿Cómo trabaja ProjectWise con Active Directory? 35

¿ProjectWise guarda mis Passwords en la Base de Datos? 36

¿ProjectWise soporta Kerberos? 36

¿Si un usuario se loguea desde el cliente Web utilizando su cuenta NT, cómo se encarga ProjectWise de la password enviada por el cable? ¿Qué protocolo se utiliza? 36

¿Si un usuario se logue desde el cliente Web utilizando su cuenta de Windows/Single Sign On, cómo se encarga ProjectWise de la password enviada por el cable? ¿Qué protocolo utiliza? 36

4.4 ProjectWise desde Afuera 36

Términos Utilizados 36

Configurando el Setup 37

Trabajando en la Extranet 37

4.5 TBD _____ **38**

4.6 TBD _____ **38**

5.0 Materiales Relacionados y de Referencia _____ **39**

1.0 Introducción a GREENBOOK

Los GreenBooks son creados por Bentley Professional Services para proveer Mejores Prácticas ya que se refieren a la utilización de las soluciones de software en el ciclo de vida de la infraestructura. Esto no sólo incluye software de Bentley, pero otros que se utilizan comúnmente en proyectos de infraestructura. Las guías se basan en la documentación de mejores prácticas realizadas por cientos de colegas de Bentley Professional Services alrededor del mundo, que han hecho a los usuarios mas eficientes en el uso de su software para infraestructura.

Los GreenBooks pueden tener varios formatos, desde una Nota Técnica, Manual de Instrucciones, White Paper, hasta Libro en formato completo. Todos los GreenBooks se proveen en formato PDF para poder descargarlo e imprimirlo. Debido a que sufren actualización constantes con nueva información, siempre se debe buscar la última revisión online.

Los GreenBooks generalmente se publican en modo Draft, en su primer revisión. Esto permite un temprano acceso a información potencial. Es por esto que los documentos Draft pueden no ser tan pulidos o pueden contener algunos errores que luego se solucionan con las revisiones mas detalladas y pulidas.

Bentley's *Be Communities* es el sistema de entrega que permite a cualquier miembro del *Be Community* descargar y utilizar Mejores Prácticas en su industria. La membrecía en el *Be Community* es sin costo. Para registrarse, visite http://communities.bentley.com. Para encontrar este GreenBook y otros, visite Be Communities y busque GreenBook.

2.0 Acerca del/los Autor(es)

Tom Atkinson es un Senior Project Manager que ha estado involucrado en Topografía (Agrimensura), Ingeniería Civil, CADD y Sistemas IT desde 1985. Ha provisto servicios relacionados con MicroStation, InRoads, InterPlot, ProjectWise y una variedad de productos raster para la comunidad de Ingeniería Civil desde 1996. Mr. Atkinson se unió a Bentley en el 2004 y ha sido responsable por el desarrollo de diseños de arquitectura de sistemas, especificaciones funcionales personalizadas, planes de implementación y planes de actualización para las soluciones de ProjectWise en los Departamentos de Transporte del Estado y Empresas de Consultoría de Ingeniería Civil en Norte América..

Kevin Boland TBD

Audrius Zimnickas TBD

3.0 Resumen del Documento

Propósito: Este documento explica cómo trabajan los Permisos de Acceso dentro de ProjectWise y los varios métodos en que se pueden aplicar a carpetas y documentos. Se proveen ejemplos de Permisos de Acceso, pero no se hace ningún intento en definir cómo una organización debería modelar sus Derechos de Acceso específicos.
Destinado A: Este documento está destinado a Administradores de ProjectWise que tengan un conocimiento básico de los siguientes componentes de ProjectWise:

- Datasources
- Environments
- Folders and Documents
- Users
- User Groups
- User List

Derechos de Acceso (Definición): La forma en que ProjectWise impone la seguridad dentro de un datasource, controlando qué usuarios pueden ver qué documentos y carpetas, y lo que esos usuarios pueden realizar con esos documentos y esas carpetas. Los términos Derechos de Acceso y Seguridad se utilizaran indistintamente a lo largo de este documento.

4.0 Conceptos de Permisos de Accesos de ProjectWise

Las carpetas y documentos pueden ser accedidos por cualquier usuario con una cuenta activa en datasource, o se los puede hacer exclusivos a ciertos usuarios a través de **access control** (control de acceso). El Control de Acceso determina qué usuarios pueden ver qué documentos y carpetas, y qué se les permite hacer a esos usuarios con los documentos y las carpetas.

La Seguridad en ProjectWise es exclusiva: Cuando se crea un datasource, no hay configuración de control de acceso definida, por lo tanto todos los usuarios creados tendrán acceso a todas las carpetas y documentos en el datasource de la siguiente forma: El grupo de Administradores tendrá Control Total, el resto de los usuarios tendrán acceso de Lectura/Escritura pero no tendrán la posibilidad de Modificar los Permisos. Sólo cuando a algunos usuarios se les da explícitamente permisos de acceso a ciertos ítems, que los otros usuarios quedarán excluidos de acceder a esos mismo ítems.

La Seguridad de puede aplicar en varios lugares: En ProjectWise Administrator, la seguridad de puede aplicar globalmente al datasource, y/o a entornos, flujos de trabajo y etapas específicas. En ProjectWise Explorer, se puede aplicar seguridad a carpetas y documentos específicos. Los varios niveles de permisos de acceso permiten controlar el acceso en forma global, a través de etapas o carpetas, o estrictamente asignando permisos a cada carpeta, flujo de trabajo y etapa. Sin importar donde se defina la seguridad, el método es básicamente el mismo: abrir el cuadro de diálogos Properties del ítem, y en el tab Folder o Documento Security agregar los usuarios a los cuales se les desea configurar la seguridad.

La configuración excesiva de seguridad puede afectar la performance: Mientras que ProjectWise puede manejar configuraciones complejas de seguridad, se debe tener en cuenta, que cuando haya menos configuraciones de seguridad, mejor será la performance, en particular cuando se crean nuevas carpetas o se modifican las configuraciones de seguridad.

Esta sección identificará los conceptos de Derechos de Acceso que aplican a ProjectWise para ambos tipos de permisos – **Seguridad del Objeto** y **Seguridad del Flujo de Trabajo** y también los permisos que se definen en **User Settings**. Estas tres áreas de control se deben considerar cuando se determinan los permisos que un individuo tiene sobre un documento en particular.

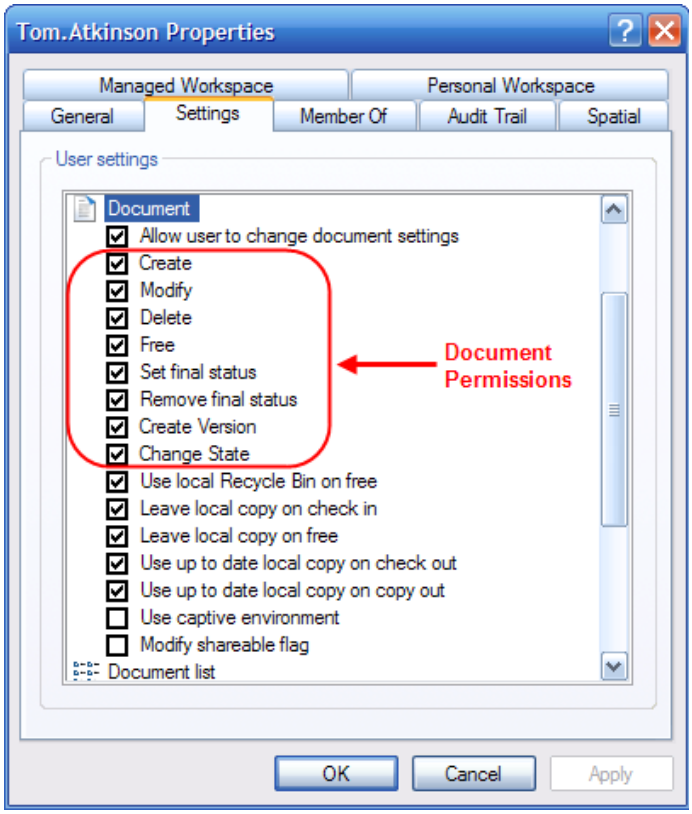
Por ejemplo, considere el siguiente proceso mental cuando se trate de determinar por qué un usuario no puede borrar un documento en particular:

- ¿El usuario tiene permisos para borrar documentos dentro de su User Settings?
- ¿La Seguridad de Objetos de ProjectWise le otorga a este usuario los permisos para borrar?
- ¿La Seguridad de Flujos de Trabajo de ProjectWise le otorga a este usuario permisos para borrar ?

No es un requerimiento que se definan derechos de acceso a un documentos por seguridad del Objeto o por seguridad del Flujo de Trabajo, pero ambos se pueden aplicar tanto a carpetas como a documentos. Sin importar la seguridad aplicada a las carpetas y documentos, si el usuario no tiene el permiso específico en su User Settings, no tendrá permisos para realizar la operación.

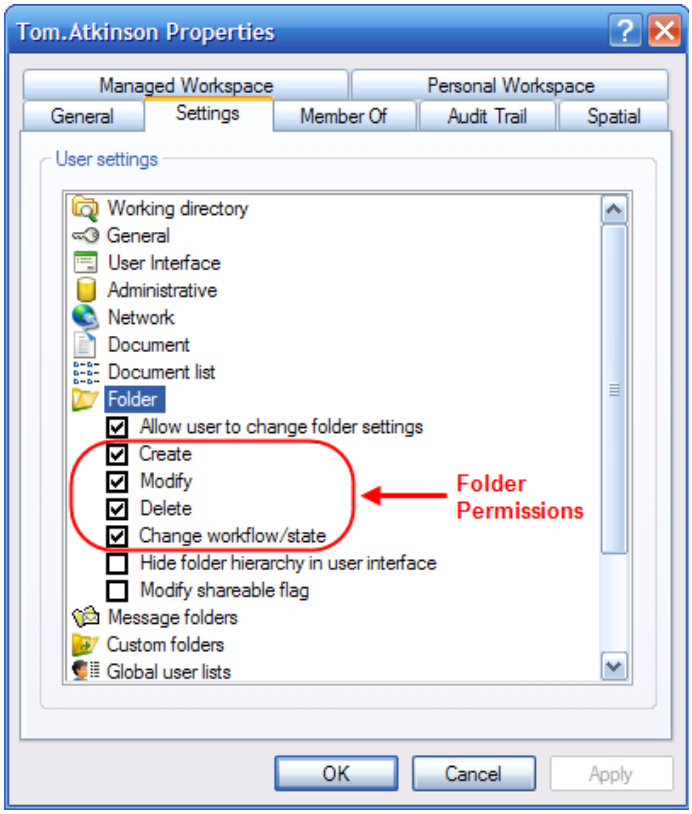
Veamos algunos de los ajustes:

Controles de Documentos (User Settings): Dentro de las propiedades de cada usuario están las opciones que controlan una gran variedad de funciones de ProjectWise. En el tab settings hay grupos de configuraciones que controlas los permisos que los usuarios tienen con respecto a documentos y carpetas. Para que los usuarios puedan Crear, Modificar, Borrar, Liberar, Definir Estado Final, Remover Estado Final, Crear Versiones o Cambiar Etapas de los documentos se les debe otorgar el permiso dentro de sus user settings. Sin estos permisos básicos, el usuario no podrá realizar estas funciones aunque tenga los derechos sobre los objetos lo permitan.



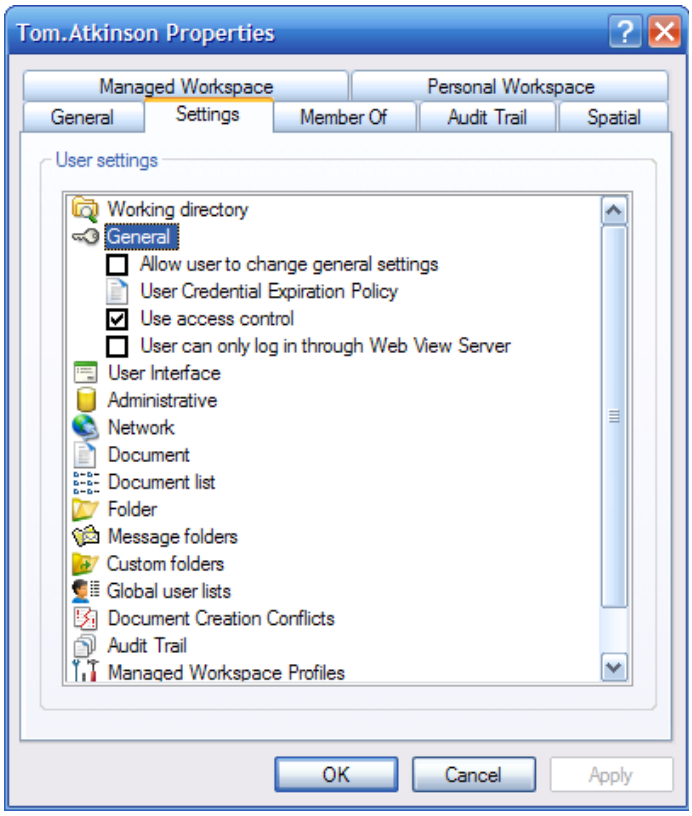
A pesar que el ajuste "Modify shareable flag" no se muestra en la imagen como un permiso de los documentos, esencialmente es porque otorga al usuario los permisos para habilitar o deshabilitar el ajuste "shareable" en el cuadro de ajustes Properties para cualquier documento V8 DGN en ProjectWise Explorer. El ajuste de Datasource "Enable shareable documents" debe estar habilitado antes de poder habilitar este ajuste de usuario. Por otra parte, si el ajuste de usuario "Allow user to change document settings" está prendido, entonces estos ajustes se presentarán al usuario y éste tendrá la habilidad de modificarlos.

Controles de Carpeta (Ajustes de Usuario): Igual que los permisos de documentos controlan qué funcionalidades el usuario tiene permiso de ejecutar en los documentos. Los permisos de Carpetas controlan si el usuario puede o no Crear, Modificar, Borrar y Cambiar Flujo de Trabajo o Etapa de una carpeta.



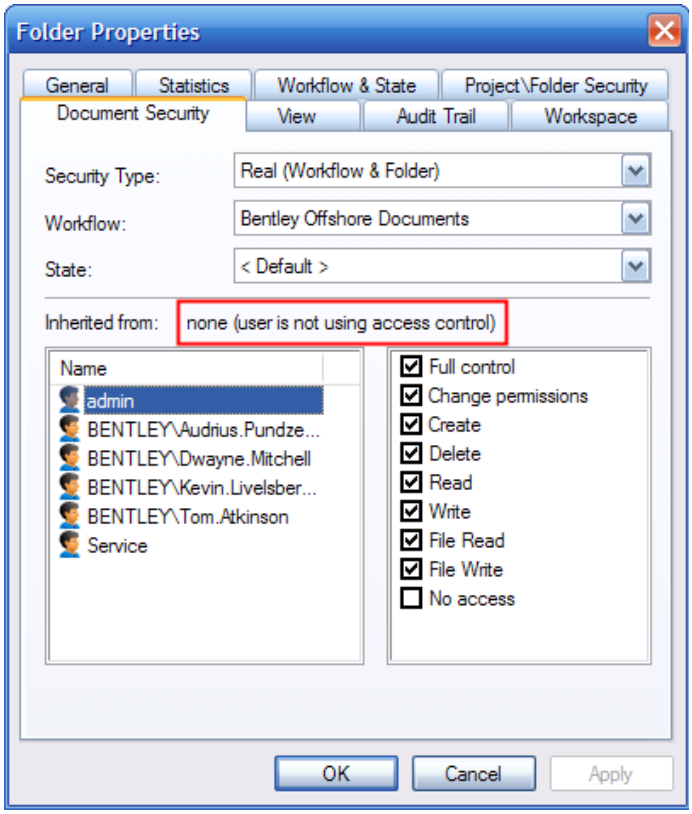
A pesar que el ajuste "Modify shareable flag" no se muestra en la imagen como un permiso de las carpetas, esencialmente es porque otorga al usuario los permisos para habilitar o deshabilitar el ajuste "shareable" en el cuadro de ajustes Properties para cualquier carpeta o proyecto en ProjectWise Explorer. El ajuste de Datasource "Enable shareable documents" debe estar habilitado antes de poder habilitar este ajuste de usuario. Por otra parte, si el ajuste de usuario "Allow user to change document settings" está prendido, entonces estos ajustes se presentarán al usuario y éste tendrá la habilidad de modificarlos.

Utilizar Control de Acceso (Ajustes de Usuario): Hay un ajuste de usuario llamado “Use access control” que se puede prender o apagar en el ProjectWise Administrator para controlar si una cuenta de usuario debe o no adherir a los ajustes de seguridad en el ProjectWise DataSource. Si se apaga este ajuste, entonces el usuario está esencialmente “inmune” a todos los ajustes de seguridad en ProjectWise sin importar cómo están definidos y tendrá control completo sobre las carpetas y documentos..

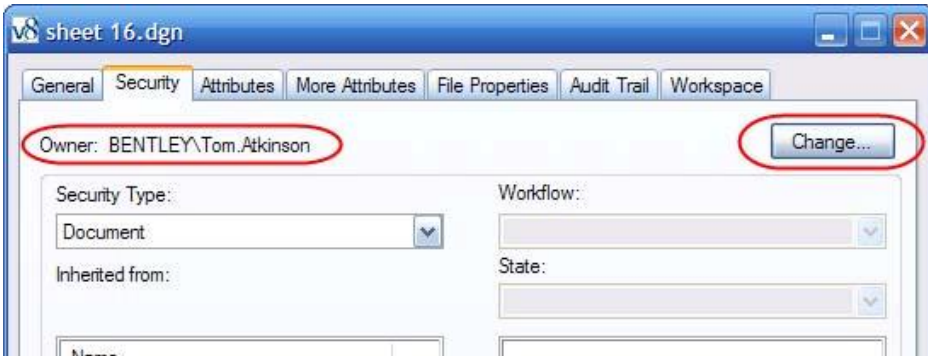


Este ajuste sólo se debe apagar para un selecto número de cuentas como para cuentas utilizadas para servicios de indexación de documentos, para asegurar la posibilidad de acceder a todos los documentos. Adicionalmente, puede ser de gran utilidad cuando un administrador se prohíbe accidentalmente de acceder a carpetas y/o documentos.

Además, todo usuario que tenga este ajuste apagado aparecerá en Tipo de Seguridad “Real” con Control Total y una nota que indica que se le conceden permisos de acceso ya que el usuario no está utilizando control de acceso.



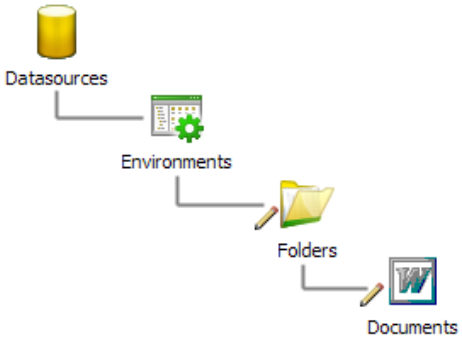
Propiedad: Un usuario que crea un documentos será el Propietario de dicho documento. Un usuario que crea una carpeta será el Propietario de la carpeta y de los documentos dentro de la carpeta. Por lo tanto, esencialmente, un documento puede tener dos usuarios que pueden ejercer los privilegios de Propiedad. Excepto cuando "No Access" se aplica al objeto para el usuario en particular – los Propietarios de un objeto tiene permisos implícitos para modificar dicho objeto. Inclusive si al usuario no se le conceden "Change Permissions", el usuario tendrá permisos de modificación si es el Propietario.



Cuando una carpeta no tiene asignado seguridad por Flujo de Trabajo, el propietario de dicha carpeta siempre tiene permisos de Modificación sobre dicha carpeta y sus sub-carpetas, en este caso, el propietario puede denegar

acceso a la carpeta inclusive a los administradores. Cuando una carpeta tiene seguridad aplicada por Flujo de Trabajo, el propietario no tiene mas permisos incondicionales de Modificación, inclusive puede perder acceso a dicha carpeta si se lo excluye en los ajustes de seguridad del Flujo de Trabajo.

Reglas de Jerarquía: ProjectWise tiene la habilidad de aplicar seguridad tanto a Carpetas como a Documento en varios niveles de la arquitectura del sistema (Datasource, Environment, Folder y Document). En el caso donde se asigna permisos de acceso a múltiples niveles, van a prevalecer los permisos que estén mas cerca del objeto que se está accediendo. Los Permisos de Acceso que están adjuntos a un objeto se refieren comúnmente como Access Control List (ACL). Las Jerarquías van subiendo hasta encontrar una sola ACL que aplique. Cuando se encuentra una ACL, sólo se tiene en cuenta dicha ACL para determinar los permisos de acceso. En otras palabras, ACL's para múltiples niveles no se "unifican".



(Los permisos de acceso definidos para documentos en el nivel de carpeta – o carpeta superior prevalecerán sobre los permisos de acceso definidos a nivel de environment o datasource).

No Access: Si el usuario tiene No Access definido para un objeto (carpeta o documento) el usuario no podrá ver dicho objeto, por lo tanto no podrá ejercer ningún derecho. El permiso "No Access" toma prioridad sobre todos los otros. Hay otro escenario (aparte de definir explícitamente "No Access") que pueden causar que un usuario tenga "No Access" para un documento. Cuando se hayan aplicado permisos de acceso a un objeto y un usuario en particular no está listado en ninguno de los usuarios, grupos, listas de usuarios o el grupo Everyone definidos en esos permisos, entonces el usuario tendrá No Access.

ProjectWise es Muy Restrictivo: ProjectWise tiene dos tipos de permisos: permisos "Allow" (autorización) y permisos "Deny" (negación). Mientras que los permisos Allow tienen cierta granularidad que especifican si un usuario puede Crear, Editar y Borrar, etc.… hay un solo permiso Deny que se llama "No Access". En el caso que un usuario pertenezca a dos grupo que tengan acceso "Allow" aplicado al mismo documento; uno con acceso sólo-lectura, el otro con acceso lectura-escritura, el usuario tendrá la suma de los permisos "Allow" que resultará en acceso lectura-escritura. Si alguno de los grupos especifica "No Access", el usuario tendrá No Access sin importar cuántos permisos "Allow" tenga el usuario.

Seguridad de Flujo de Trabajo vs Seguridad del Objeto: La Seguridad de Flujo de Trabajo aplica tanto a carpetas como a documentos y los derechos de acceso se pueden aplicar a nivel de Flujo de Trabajo como a nivel de Etapa dentro de Flujo de Trabajo (los permisos de acceso definidos en cualquiera de los niveles se llaman Seguridad de Flujo de Trabajo). La seguridad de Flujo de Trabajo prevalecerá sobre la Seguridad del Objeto para los objetos en dicho Workflow/State a menos que se especifique "No Access" para el objeto. Cuando se defina seguridad de Flujo de Trabajo, entonces los permisos de acceso definidos a nivel Etapa prevalecerán sobre los permisos de acceso definidos a nivel Flujo de Trabajo.

4.1 Seguridad del Objeto

Esta sección identificará las propiedades de seguridad que aplican a ProjectWise utilizando el método de Seguridad del Objeto.

Herencia de la Seguridad del Objeto

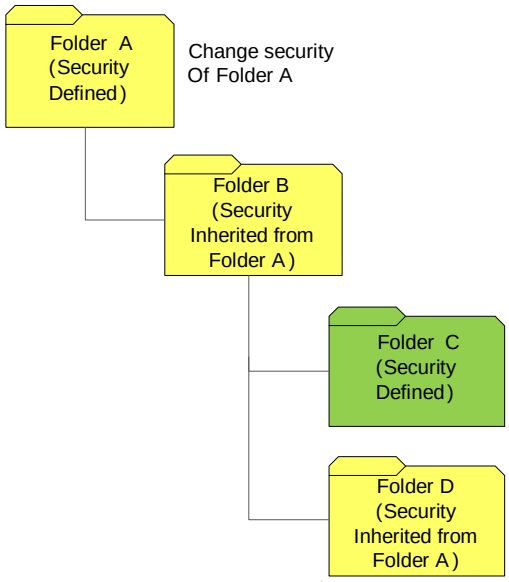
Las Carpetas pueden heredar la seguridad desde otras carpetas que están mas arriba en la jerarquía o pueden tener definida explícitamente su propia seguridad. Cuando un Administrador de ProjectWise aplica cambio a la seguridad de una carpeta, el o ella también puede cambiar la seguridad de las sub-carpetas que existen debajo de la misma. Cuando se realizan modificaciones a la seguridad de una carpeta que tiene sub-carpetas, se presenta un cuadro de diálogos que permite al usuario aplicar los cambio sólo a dicha carpeta o a todas las sub-carpetas.

Confirm Folder Security Changes
You have chosen to change the folder's permissions. Do you want to apply this change to this folder only, or do you want to apply it to subfolders also? Applying change for subfolders will remove their current permissions.
Apply changes to this folder only (subfolders may still inherit them)
Apply changes to this folder and subfolders
OK
Cancel

Si una carpeta tiene sub-carpetas, seleccionar "**Apply changes to this folder only**" afecta la seguridad de la carpeta seleccionada y la de sus sub-carpetas de la siguiente forma:

- Las sub-carpetas que hereden la seguridad de la carpeta modificada (no tienen ninguna definición de seguridad) ahora reflejarán los cambios realizados.
- Las sub-carpetas que tienen su propia seguridad no se verán afectadas por estos cambios.

Diferentes resultados aplicarán dependiendo en la opción seleccionada. Veamos el primer escenario donde el usuario selecciona "Apply changes to this folder only".



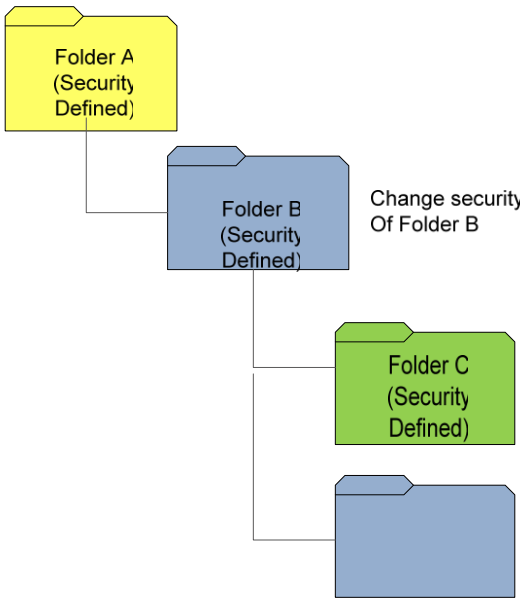
Este diagrama muestra una estructura de carpetas donde la carpeta de arriba (**Folder A**) tiene su propia seguridad y todas las sub-carpetas heredan esta seguridad excepto la carpeta **Folder C**.
Si se realiza una modificación a la seguridad de **Folder A y** se selecciona "**Apply changes to this folder only**", los nuevos ajustes no se aplicarán a las carpetas que tengan definida su propia seguridad (como la carpeta **Folder C**). Sin embargo las otras carpetas (**Folders B and D**) heredan la seguridad de la carpeta **Folder A** por lo tanto la seguridad será actualizada para reflejar los nuevos ajustes.

Las carpetas que heredan seguridad, heredarán la seguridad de la carpeta mas cercana en la jerarquía que tenga definida su propia seguridad. Veamos un leve variación al ejemplo previo.

Cuando se modifica la seguridad a una sub-carpeta **(Folder B)** que hereda su seguridad de una carpeta padre y se selecciona "**Apply changes to this folder only**" pasa lo siguiente:

1. No se afectarán las sub-carpetas que tengan su propia seguridad.
2. Todas las sub-carpetas debajo de la carpeta modificada que heredan su seguridad de una carpeta superior, ahora heredarán su seguridad de la carpeta que fue modificada.

Veamos qué pasa si se modifica la seguridad de **Folder B** y se selecciona "**Apply changes to this folder only**".



En este diagrama tenemos la misma estructura de carpetas mostrada en el Diagrama en la página anterior.
Hemos cambiado la seguridad en la carpeta **Folder B** para que ahora tenga su propia seguridad. Hemos seleccionado la opción "**Apply changes to this folder only**" y los resultados se muestran en el diagrama de la izquierda.
Tomar nota que **Folder C** retiene su propia seguridad igual que en el ejemplo previo pero **Folder D** ahora hereda su seguridad de la carpeta **Folder B** en lugar que de **Folder A**. Esto es porque **Folder B** está mas cerca de **Folder D** que de **Folder A**. Si hay otras sub-carpetas en el mismo nivel que **Folder B**, seguirán heredando de **Folder A**.

Cuando se planifique el modelo de seguridad, generalmente es mejor definir permisos de acceso por defecto a las carpetas superiores y aplicar esos ajustes a todas las sub-carpetas. Luego comenzar al final de la estructura de carpetas para definir permisos de accesos sólo a las carpetas que lo requieren – tener en cuenta que todas las sub-carpetas ahora heredarán los permisos de acceso desde la carpeta recientemente modificada.

¿Qué pasaría si en el ejemplo, un Administrador modifica los permisos de acceso a **Folder A** y selecciona "Apply changes to this folder and subfolders"? Cuando se selecciona dicha opción se removerán todos los ajustes de seguridad de todas las sub-carpetas y ahora heredarán la seguridad de la carpeta **Folder A**.

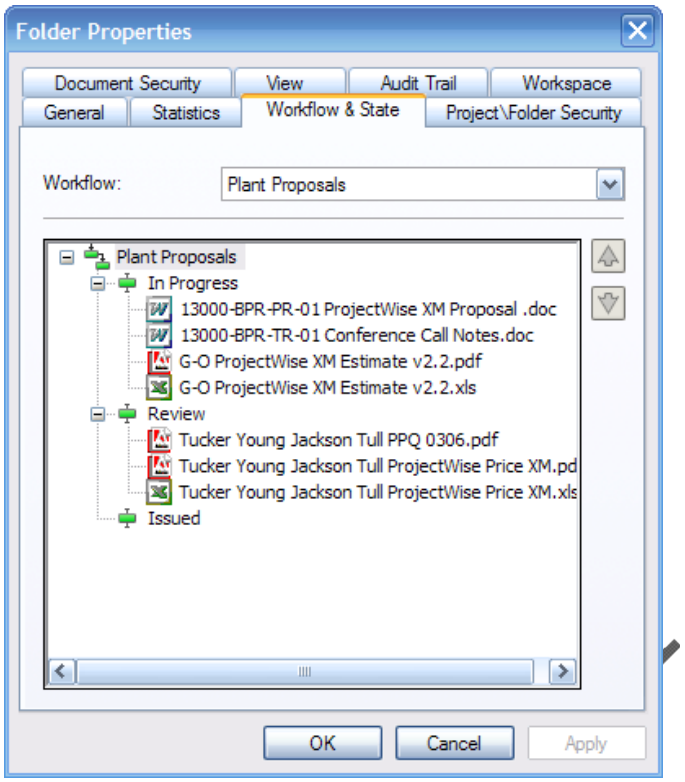
4.2 Seguridad de Flujo de Trabajo

A medida que los proyectos progresan en su ciclo de vida, es común que se agreguen nuevos usuarios a los equipos y también que algunos usuarios se remuevan de los equipos. Por esta razón, la seguridad debe ser flexible y se debe ajustar en hitos específicos. Esta sección examinará cómo los ajustes de Seguridad de Flujos de Trabajo pueden hacer que sea sencillo modificar la seguridad en las carpetas o documentos cuando alcanzan ciertos hitos.

El siguiente diagrama representa un simple flujo de trabajo de tres etapas. Si se va a introducir un flujo de trabajo a un equipo de trabajo, probablemente será un nuevo proceso para que ellos sigan y por lo tanto cuanto mas simple el flujo de trabajo, mayor posibilidad de éxito. Los Flujos de Trabajo con muchas etapas pueden confundir a la gente a tal punto que no sepan a qué etapa debería pertenecer un documento.

State name	State description
In Progress	In Progress
Review	Review
Issued	Issued

Dentro de ProjectWise Explorer, los usuarios pueden ver qué documentos están en qué etapa a través del tab "Workflow & State" de las Propiedades de Carpeta, como se muestra a continuación.



Seguridad de Flujo de Trabajo: Los Permisos de Acceso se pueden aplicar a cada Etapa dentro de un Flujo de Trabajo para tanto Carpetas como Documentos. Si una Carpeta o Documento tienen permisos de acceso asignados tanto por Seguridad de Objeto y por Seguridad de Flujo de Trabajo, entonces prevalecerá la Seguridad de Flujo de Trabajo, excepto en el caso que la Seguridad de Objeto resulte en No Access:

Ejemplo 1:

- La Seguridad de Objeto define Sólo-Lectura sobre documento A para el Grupo A
- La Seguridad sobre la Etapa del Flujo de Trabajo define Lectura-Escritura sobre documento A para el Grupo A.

Resultado: El Grupo A tendrá permiso de Lectura-Escritura sobre el documento A (gana el Flujo de Trabajo).

Ejemplo 2:

- La Seguridad de Objeto define Lectura-Escritura sobre el documento A para el Grupo A.
- La Seguridad sobre la Etapa del Flujo de Trabajo define Sólo-Escritura sobre el documento A para el Grupo A.

Resultado: El Grupo A tendrá permiso de Sólo-Lectura sobre el documento A (gana el Flujo de Trabajo).

Ejemplo 3:

- La Seguridad del Objeto define No Access sobre el documento A para el Grupo A.

- La Seguridad sobre la Etapa del Flujo de Trabajo define Lectura-Escritura sobre documento A para el Grupo A.

Resultado: El Grupo A tendrá No Access y no podrá ver el documento A (gana No Access)

Ejemplo 4:

- La Etapa del Flujo de Trabajo define Lectura-Escritura sobre el documento A para el Grupo A.
- La Etapa del Flujo de Trabajo define Sólo-Lectura sobre el documento A para el Grupo B.
- La Seguridad de Objeto define Lectura-Escritura sobre documento A para el Grupo C, pero…..
- El Grupo C no está listado en el tab de Seguridad del Documento para el Flujo de Trabajo

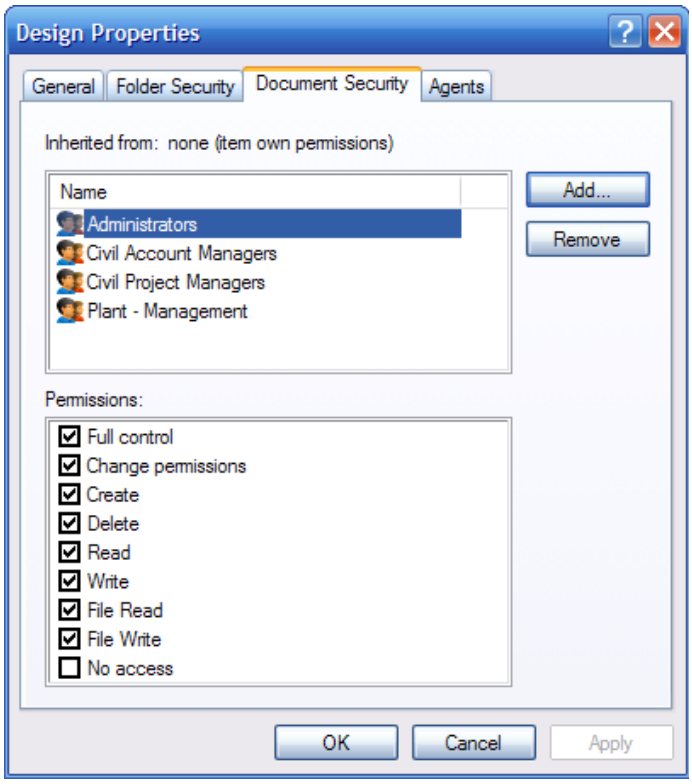
Resultado: El Grupo C tendrá No Access al documento y ni siquiera lo podrá ver.

Resumen:

- El ajuste "No Access" ganará sobre todos los otros ajustes así sea definido en una Etapa del Flujo de Trabajo o directamente en una Carpeta a través de la Seguridad de Objeto.
- Cuando está en juego la Seguridad de Flujo de Trabajo, sólo aquellos usuarios a los que se les otorga permisos tendrán permiso de acceso, todos los otro tendrán No Access.

Tener en cuenta que un Flujo de Trabajo no necesita tener permisos de acceso para nada – es una característica opcional de los Flujos de Trabajo. Alguno usuarios aplican Flujos de Trabajo a las carpetas simplemente para rastrear la etapa de los documentos pero no requieren modificaciones de seguridad. Cuando no se definen entradas en el tab seguridad de un flujo de trabajo, el flujo de trabajo impactará en los permisos de acceso existente y la Seguridad de Objeto tendrá efecto.

Aplicando Seguridad de Flujo de Trabajo: Los Permisos de Acceso se pueden definir cuando se crea un Flujo de Trabajo en ProjectWise. Se pueden definir en cada Etapa del Flujo de Trabajo pero también a nivel del Flujo de Trabajo. La siguiente imagen muestra que el grupo de Administradores tiene control total para Documentos a nivel de Flujo de Trabajo en el Flujo de Trabajo "Design".



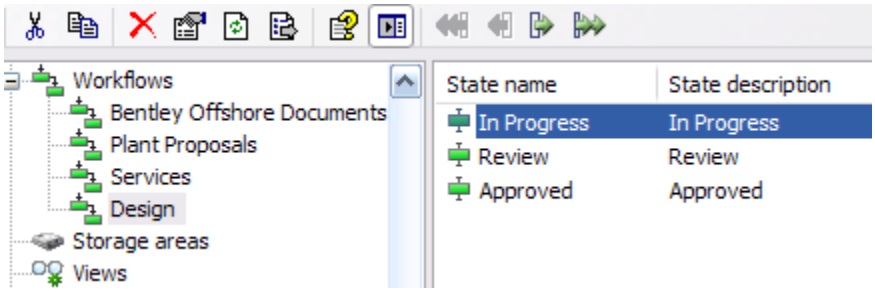
Definir la seguridad a nivel del Flujo de Trabajo puede ser ideal al componer el Flujo de Trabajo, porque cada Etapa heredará estos ajustes a medida que se vayan agregando al Flujo de Trabajo. La Seguridad para las Etapas se pueden modificar posteriormente y los cambios quedarán para la definición de la Etapa.. That is to say that the State will have its own security and will not inherit from the Workflow anymore. If a State within a Workflow is later modified to have all security settings removed then the access rights defined at the Workflow level will be reapplied through inheritance.

Seguridad Global de Flujo de Trabajo, Seguridad de Flujo de Trabajo Modificada y Herencia: La Seguridad de Flujo de Trabajo se puede definir a nivel del DataSource (en ProjectWise Administrator cuando es creado) – esto se puede llamar *Seguridad Global de Flujo de Trabajo*. La Seguridad de Flujo de Trabajo se puede modificar una vez que se haya asignado a una carpeta para controlar los permisos de acceso a diferentes grupos de usuarios – esto se puede llamar Seguridad de Flujo de Trabajo Modificada. Cuando se aplica Flujo de Trabajo a una carpeta – los ajustes de Seguridad de Flujo de Trabajo se heredarán automáticamente de la "definición" de Flujo de Trabajo mas cercana. Esto puede ser de una carpeta superior en la jerarquía o del Datasource en si mismo. Se examinará esto mas adelante.

Seguridad Global de Flujo de Trabajo: Digamos que el administrador define permisos de acceso para las carpetas y documentos en cada Etapa de un Flujo de Trabajo en ProjectWise. Cuando se aplica un Flujo de Trabajo a una carpeta, los ajustes de seguridad se aplican inmediatamente a la carpeta y a los documentos por lo tanto ahora están utilizado Seguridad de Flujo de Trabajo. Esto define un modelo de seguridad "default" o Seguridad Global de Flujo de Trabajo donde los permisos del Flujo de Trabajo se heredan del DataSource.

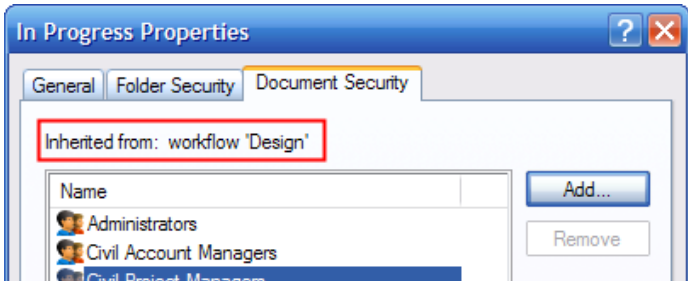
Considerar el siguiente ejemplo:

Se crea un flujo de trabajo llamado “Design” con tres Etapas: In Progress, Review y Approved.

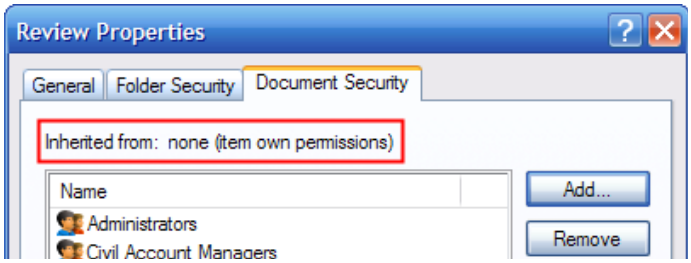


Se definieron permisos para las Carpetas y Documentos a nivel del Flujo de Trabajo “Design” de forma tal que cuando se agregue cada Etapa al Flujo de Trabajo estas heredarán automáticamente los permisos del Flujo de Trabajo.

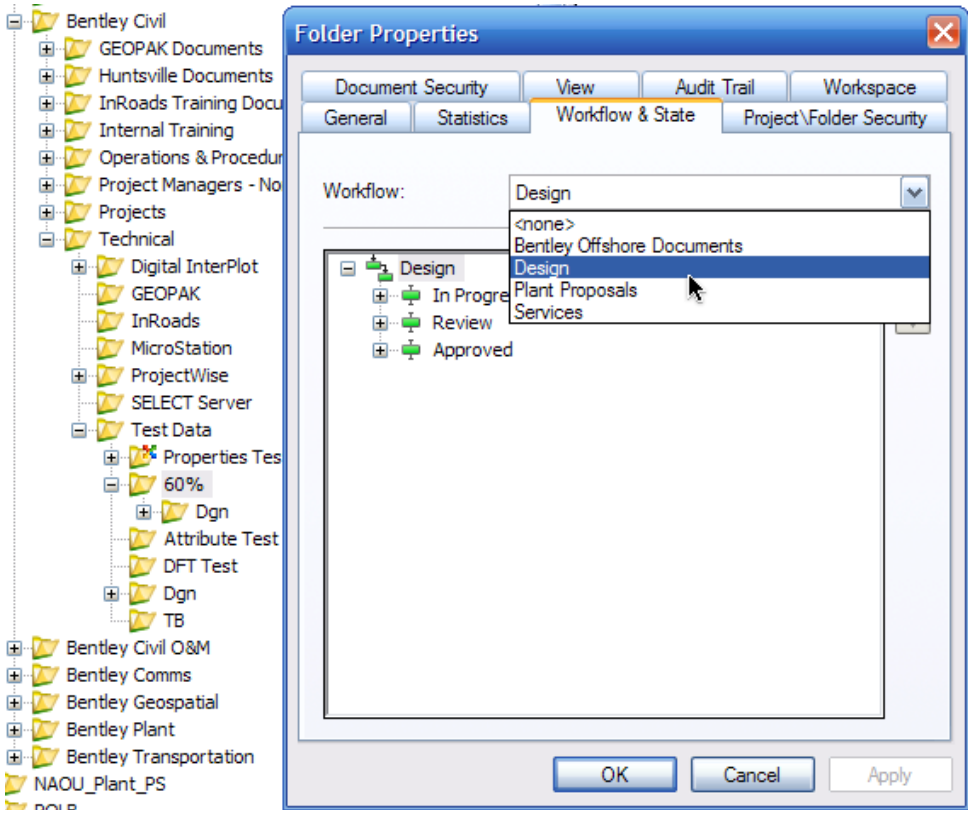
- La etapa “In Progress” no tiene cambio en sus permisos por lo tanto los Documentos y Carpetas en esta Etapa continúan heredando los permisos del Flujo de Trabajo Design.



- Las etapas “Review” y “Approved” tiene modificaciones por lo tanto definen permisos específicos a Etapa para los Documentos y Carpetas en estas Etapas.



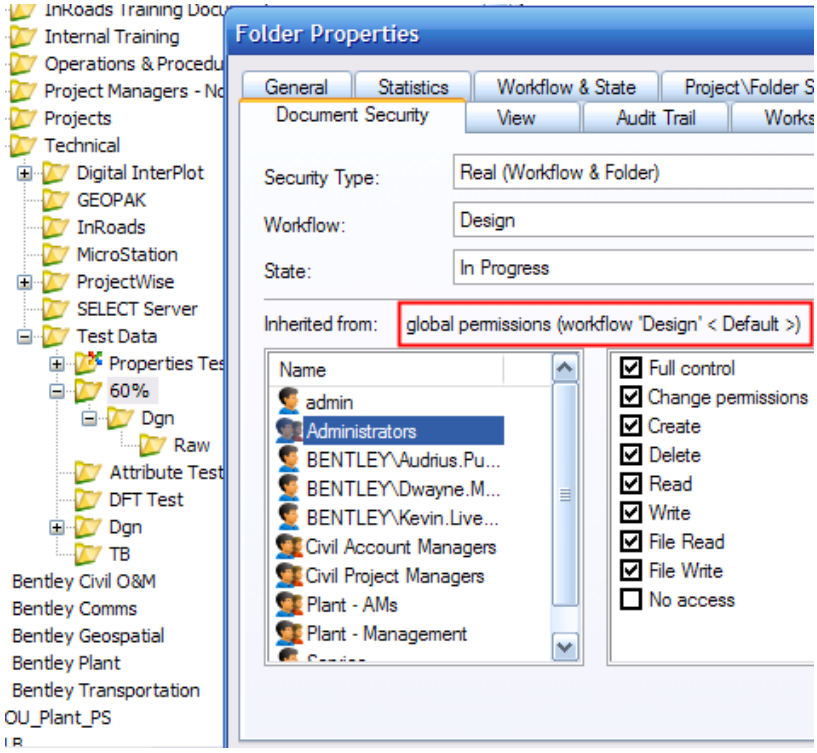
Cuando se aplica un Flujo de Trabajo a una carpeta en ProjectWise (en este caso, la carpeta 60%) se puede observar que la seguridad del Documento está controlada por el Flujo de Trabajo.



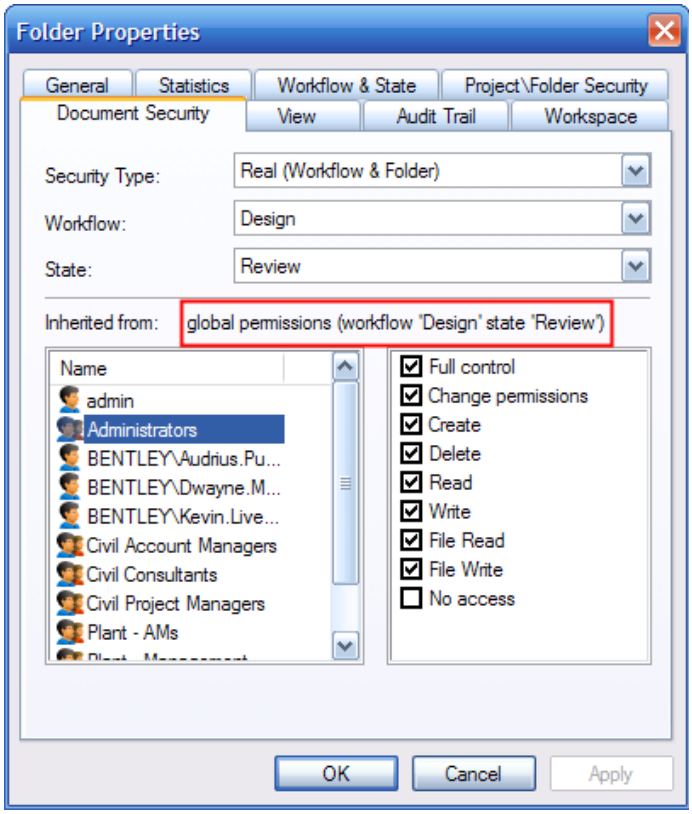
Notar que en la imagen siguiente se pueden ver tres tipo diferentes de seguridad: Real, Folder o Workflow.

- La opción **Folder** muestra qué Permisos de Objeto están activos y si son heredados de la carpeta anterior, environment o datasource – o si el objeto tiene sus propios permisos.
- La opción **Workflow** muestra qué Permisos de Flujo de Trabajo están activos para los objetos en el Flujo de Trabajo y Etapa actual. También muestra si el objeto tiene sus propios Permisos de Flujo de Trabajo o si esos permisos se heredan desde la carpeta anterior (que tiene una definición de modificación de Flujo de Trabajo aplicado) o de la definición global en el DataSource.
- La opción **Real (Workflow & Folder)** muestra el resultado de seguridad de Flujo de Trabajo/Etapa y Objeto combinadas reflejando cuál está actualmente en efecto sobre los objetos (los Permisos de Acceso no se pueden modificar si el Type está en Real). Cuando se aplica un Flujo de Trabajo a una carpeta es común ver usuarios y grupos en la lista de tres fuentes diferentes:
    1. Usuarios/Grupos/Listas que están definidas dentro de los ajustes de seguridad Flujo de Trabajo/Etapa (pero Flujo de Trabajo generalmente prevalece sobre seguridad de Objeto – excepto cuando se define “No Access”)
    1. Usuarios/Grupos/Listas que tienen definido “No Access” definido dentro de la Seguridad de Objeto (porque “No Access” siempre prevalece sobre cualquier permiso)
    2. Usuarios que tienen “Use Access Control” apagado.

En este ejemplo, los permisos de Documento de la carpeta 60% muestra que el grupo de Administradores tienen Control Total sobre los objetos en la Etapa “In Progress” State del Flujo de Trabajo “Design” a través de permisos definidos a nivel del Flujo de Trabajo Design. Dado que el ajuste en la Etapa está definido para la primer Etapa “In Progress”, que hereda los permisos desde el Flujo de Trabajo Design (porque no tienen sus propios permisos) se verán los permisos listados como “inherited from: global permissions (workflow ‘Design’ <Default>)”.



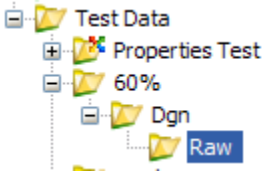
Cuando se modifica la Etapa a “Review”, que no tiene sus propios permisos de Etapa, se verá que el cuadro de diálogo se actualiza para reflejar esto:



Seguridad Modificada de Flujos de Trabajo: Supongamos que un Administrador determina que los permisos de objeto en el flujo de trabajo Design se deben alterar para un objeto en particular. El Flujo de Trabajo está definido en múltiples carpetas a través de todo el sistema para por lo tanto no se desean cambio en otros proyectos o a nivel global en el Datasource. Hay dos opciones:

1) Crear un nuevo flujo de trabajo y definir los permisos como se requieren, o
2) Aplicar el flujo de trabajo Design a la carpeta y modificar los permisos allí mismo. Esta sección se enfoca en los efecto de la opción 2.

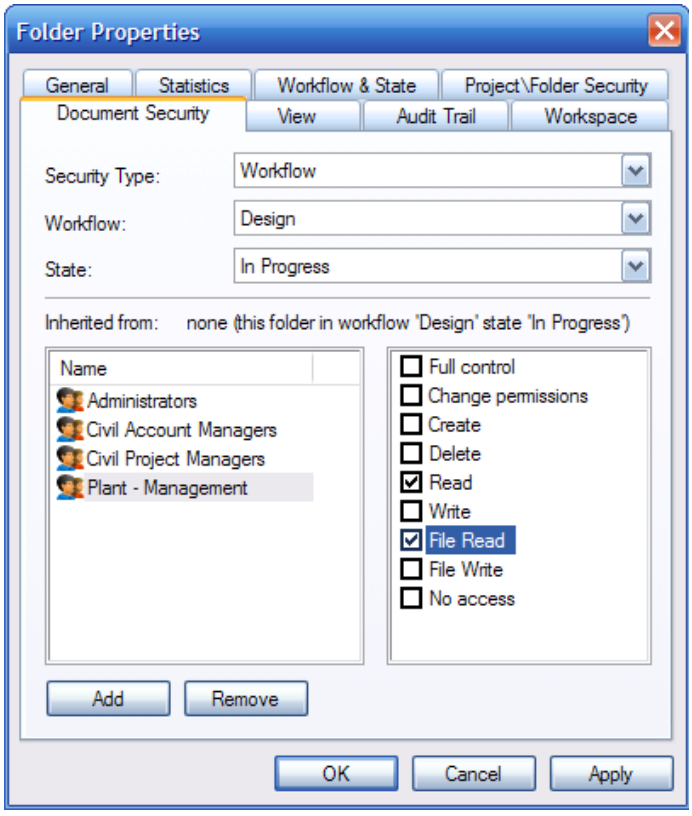
El Flujo de Trabajo Design Workflow está aplicado en la carpeta 60% pero ahora también está aplicado en la sub-carpeta llamada “Raw”.



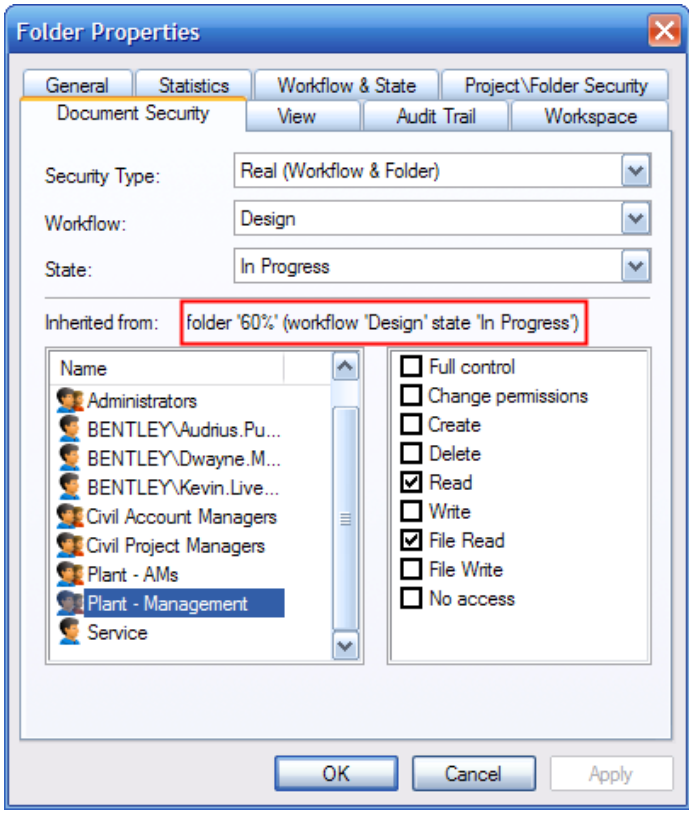
En la carpeta 60% se modificarán los permisos en la Etapa “In Progress” State para que el grupo Plant – Management tenga permisos de Lectura-Escritura en lugar de “No Access”. Cuando se aplique este cambio se le presentará al usuario el cuadro de diálogos “Confirm Folder Security Changes” como explicado anteriormente en la sección Seguridad de Objeto. Se seleccionará “Apply changes to this folder only” option.

Confirm Folder Security Changes
You have chosen to change the folder's permissions. Do you want to apply this change to this folder only, or do you want to apply it to subfolders also? Applying change for subfolders will remove their current permissions.
Apply changes to this folder only (subfolders may still inherit them)
Apply changes to this folder and subfolders
OK
Cancel

Tener en cuenta que los permisos no se heredarán mas pero ahora están definido en la etapa “In Progress” como está definido en esta carpeta.



Si se va a la sub-carpeta “Raw” y se revisa la seguridad del Documento, se verá que está heredada de la carpeta “60%”. Esto es porque ambas carpetas tienen aplicado el mismo Flujo de Trabajo y la carpeta superior (60%) tiene algunas definiciones explícitas.



Dado que las otras Etapas no han sido modificadas, si cambiamos a otra etapa (Approved, por ejemplo) se verá que los permisos de acceso para esa etapa seguirá diciendo “inherited from: global permissions (workflow ‘Design’ state ‘Approved’). Si el Administrador modifica los permisos del Flujo de Trabajo aplicado a la carpeta 60% Folder a nivel del Flujo de Trabajo (no sólo a nivel de Etapa) entonces todas las Etapas dentro del Flujo de Trabajo que no tengan definidos permisos propios, heredarán desde la definición de Flujo de Trabajo en la carpeta 60%.

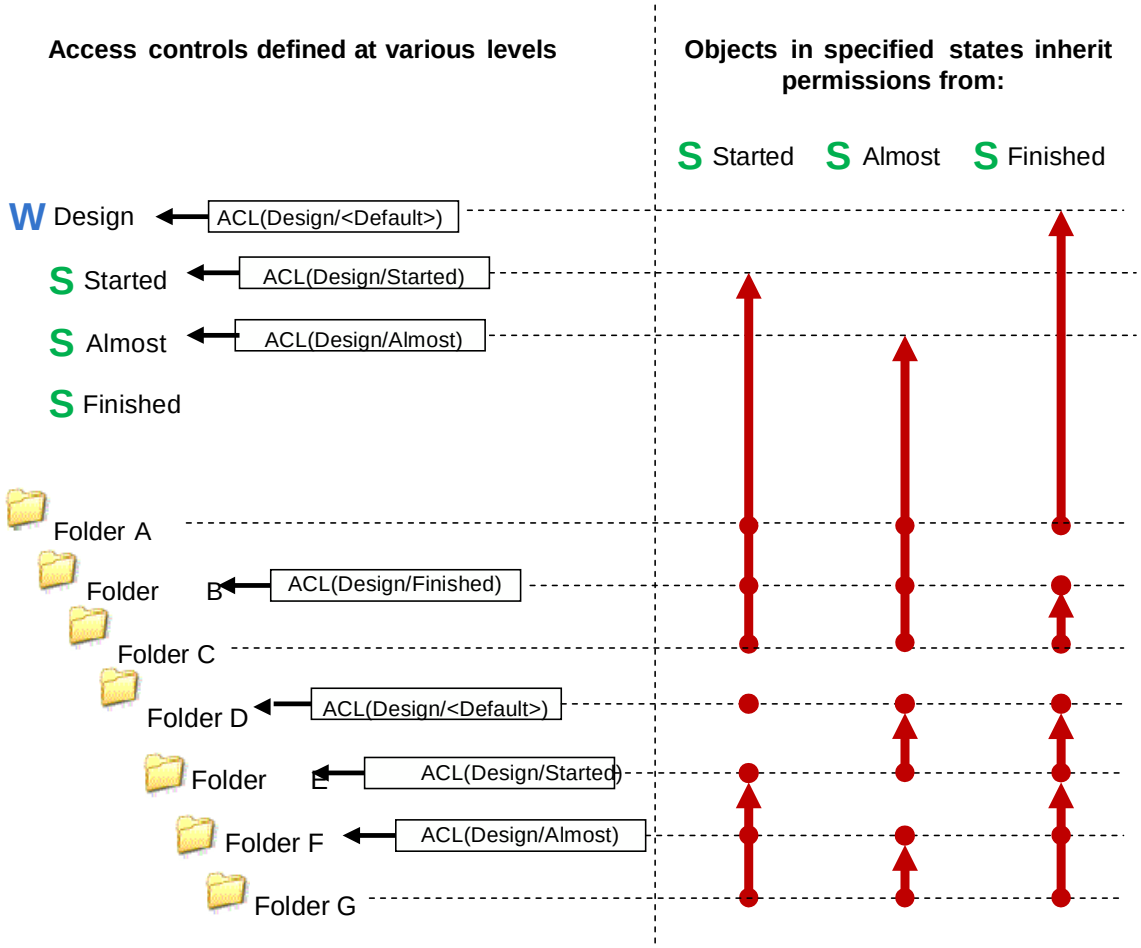
Se debe entender que la seguridad de Flujo de Trabajo que se aplica a una carpeta y luego se modifica, persistirá con esa carpeta – incluso si se remueve el Flujo de Trabajo de dicha carpeta. Por ejemplo, el Administrador abre las propiedades de la carpeta 60% , selecciona el tab Workflow & State y selecciona <none> para el Flujo de Trabajo (se ha removido el Flujo de Trabajo). Si se examina la Seguridad de Documento en la carpeta 60% ahora reportará los resultados de Seguridad de Objeto (por que hay Flujo de Trabajo definido). Sin embargo, la sub-carpeta “Raw” seguirá reportando los mismo resultados vistos en las imágenes anterior porque todavía está utilizando la Seguridad de Flujo de Trabajo y los permisos del Flujo de Trabajo “Design” estas aún definidas para la carpeta 60% a pesar que no esta aplicado. Se puede decir que la seguridad de Flujo de Trabajo está **definido** para la carpeta 60& pero no está **aplicada** a la misma. Cualquier sub-carpeta que aplique el flujo de trabajo heredará la seguridad de la carpeta 60%.

Por lo tanto una carpeta puede ser “portadora” de Seguridad de Flujo de Trabajo sin que ésta la afecte. – parecido a una persona que puede ser portadora de una enfermedad pero no estar afectada por la misma.. La carpeta tiene la

definición de Access Control List (ACL) para le Flujo de Trabajo/Etapa a pesar que dicho Flujo de Trabajo no esté aplicado a la carpeta, el ACL asociado con el Flujo de Trabajo/Etapa puede controlar la seguridad de los objetos de las sub-carpetas que están en la misma Etapa.

La forma de remover la definición de seguridad en la carpeta 60% es re-aplicar el Flujo de Trabajo Design a la carpeta y luego seleccionar Seguridad de Documento y definir Tipo de Seguridad a Workflow. Seleccionar la Etapa "In Progress" porque esta es la etapa que fue modificada. (Esto se puede verificar seleccionando un grupo y examinanda el campo "inherited from" y asegurarse que diga "none"). En este punto se deben seleccionar todos los grupos y removerlos de la lista. Cuando se cliquee el botón Apply y se acepte el cuadro de diálogos "Confirm Folder Security Changes" el administrador observará que la lista de usuarios se repoblará con la definición de seguridad global definida en ProjectWise Administrator a nivel de Datasource. La sub-carpeta "Raw" dejará de heredar los permisos de Flujo de Trabajo desde la careta 60% folder y ahora los heredará desde el datasource.

Examinaremos cómo diferentes Seguridades de Flujo de Trabajo aplican a objetos actualmente el las Etapas de un Flujo de Trabajo específico.



En la figura de arriba se tienen un flujo de trabajo "Design" con su propia lista de acceso. También se tienen 3 etapas, 2 de ellas con control de acceso definido, y 1 no (hereda del flujo de trabajo). Luego se tiene una jerarquía de carpetas, con una variedad de modificaciones al control de acceso.

***Nota**: Se asume que puedan existir otros flujos de trabajo en el datasource, pero cuando hablamos acerca de permisos de usuarios a Documentos o Carpetas actualmente en algunas etapas del flujo de trabajo, la existencia de otros flujos de trabajo no tienen influencia en los permisos calculados, por lo tanto es suficiente evaluar el acceso a un flujo de trabajo por vez, ignorando todos los otros flujos de trabajo.*

***Nota**: En este ejemplo se asume que se habla tanto de acceso a Documentos o Carpetas, dado que estos sistemas de seguridad son independientes y aplican igualmente a cualquiera de ellos.*

***Nota**: Cada una de las carpetas listadas pueden tener o no tener control de acceso para Seguridad de Objeto, o para otros flujos de trabajo y etapas. No tienen influencia, lo mismo que no existiesen.*

Examinemos algunos casos:

- Carpeta A. Esta carpeta no define ningún control de acceso para este flujo de trabajo, por lo tanto los objetos en cualquier etapa del flujo de trabajo heredarán el control de acceso del datasource – amplio control de acceso especificado en los niveles de flujo de trabajo y etapas.
- Carpeta B. Esta carpeta tiene control de acceso que define el acceso a los objetos en la etapa "Finished", por lo tanto los objetos en esta etapa tendrán acceso específico, y los objetos en otras etapas heredarán el control de acceso del datasource – amplio control de acceso especificado en los niveles de flujo de trabajo y etapas.
- Carpeta C. Esta carpeta no tiene definido control de acceso para este flujo de trabajo, por lo tanto los objetos en cualquier etapa del flujo de trabajo heredarán el control de acceso. Los objetos en la etapa Finished heredará de la carpeta B, los objetos en otra etapas del datasource – amplio control de acceso.
- Carpeta D. Esta carpeta tiene definido un control de acceso para todas las etapas del flujo de Trabajo Design, por lo tanto los objetos en cualquier etapa de este flujo de trabajo obtendrán el mismo acceso de la carpeta D. Además, todas las sub-carpetas de Carpeta D heredarán el acceso para los objetos actualmente en cualquier etapa desde Carpeta D.

¿Cómo se determinan los permisos de acceso?

Cuando se debe determinar el acceso a objetos específicos, tanto de Documento como de Carpeta, el control de acceso se determina de acuerdo al siguiente algoritmo:

Acceso a Objetos vía "Seguridad de Objeto" se calcula, examinando la jerarquía del objeto. Si (**Acceso a Objeto** resulta en **No Access**)

Entonces

El usuario tiene **No Access**

Si no

Acceso a Flujo de Trabajo vía "Seguridad de Flujo de Trabajo" se calcula, examinando la jerarquía del objeto.

Si (**Acceso a Flujo de Trabajo** se niega para objetos en esta etapa

Entonces

Si no

El usuario tiene acceso igual al calculado para **Acceso a Workflow**

El usuario tiene acceso igual al calculado para **Acceso a Objeto**

También es importante cambiar el pensamiento de definición de acceso a lógica de cálculo de acceso cuando se trata de entender cómo funciona el control de acceso. Durante el tiempo de acceso, un objeto está participando en una etapa de un solo flujo de trabajo o no está participando de ningún flujo de trabajo. Si el objeto está participando en una etapa entonces ningún otro flujo de trabajo o etapa tendrán influencia en el acceso al objeto.

El examen de jerarquía se realiza examinando los nodos de jerarquía escalando hacia arriba. En cada paso se realiza una resolución importante.: Así sea que el nodo tenga controles de acceso "aplicables" o no. Si tiene – el escalado termina en el siguiente escalón, si no – continúa. Si un nodo sólo tiene entradas no-aplicables de Access Control List (ACL), se lo considerará como que no tiene ningún ACL. Por ejemplo, si una carpeta sólo tiene entradas específicas a seguridad de Objeto, ese nodo se considerará que no tiene ACL cuando se realicen exámenes específicos a flujo de trabajo.

Sería útil pensar que el código de determinación de Seguridad de Objeto "tiene anteojos especiales" y sólo ve controles de acceso que son independientes del flujo de trabajo. Y que e código de determinación de Seguridad de Flujo de Trabajo sólo ve el control de acceso aplicado a la etapa específica del flujo de trabajo en la que se encuentra el documento.

Security Type	Hierarchy	Applicable entries	Non-applicable Entries
Object Access	Datasource Environment Folder(s) Document	Non-workflow specific entries	Entries for any specific workflow or for any specific workflow state
Workflow Access	Workflow Workflow State Folder(s) Document	Entries for a specific workflow state, and entries for a specific workflow and a <default> state	Non-workflow specific entries. Entries for a different workflow. Entries for a different workflow state.

Pero también hay Ajuste de Usuario - ¿cómo entran éstos en juego?

Dadas todas estas reglas ahora podemos ver cómo la Seguridad de ProjectWise determina qué tipo de permisos de acceso se le otorgan a un usuario en particular. Entre los ajustes Globales y los ajustes de Carpeta, ajustes de Flujo de Trabajo y ajustes de Usuario, la única forma posible de determina esto sería mirar a la lógica detrás del mismo. Tener en cuenta que la lógica puede considerar escenarios que no son considerados "mejores prácticas". Por ejemplo, la lógica a continuación menciona a usuarios individuales identificados en la lista de acceso. Muchos administradores consideran como "mala práctica" utilizar individuos (en lugar de grupos) en el modelo de seguridad actual, porque se torna muy difícil de administrar.

La lógica se a dividido en dos conjuntos, uno para el nivel que se refiere a los Ajustes de Usuario para el Control de Acceso y otro que explica el proceso de determinar los derechos de acceso una vez que se establecieron dichas condiciones. Se presenta esta lógica para ayudar a los Administradores de ProjectWise a comprender que se debe considerar cuando se definen los derechos de acceso – no necesariamente cómo ProjectWise procesa estos ajustes desde una perspectiva informática.

First, we must consider the User Settings:

Si (el ajuste "Use Access Control" está apagado)
Entonces
    El usuario tiene Control Total
Si no
    El usuario tiene Permisos definidos en Ajustes de Usuario (Carpeta & Documento)

A continuación, se examinará la Seguridad de Objeto para ver si definió "No Access" para el usuario– si es así el usuario tendrá No Access. Se examinará la jerarquía para determinar dónde está la lista de control de acceso mas cercana. Aquí es de donde vendrán los permisos y se pueden definir explícitamente en el objeto o en algún lugar anterior. Una vez establecido, ProjectWise buscará si se definió No Access para el Usuario, luego en cualquier Grupo donde esté el usuario, luego en las Listas de Usuarios, luego en Grupo Everyone.

La lógica sería así::

Si (el usuario está mencionado en la lista de acceso)
Entonces
    Si (se definió No Access para dicho usuario)
    Entonces
        El usuario tiene No Access
    Si no
    El usuario tiene accesos definido para él mismo
Si no
    Si (hay Grupos donde se lo menciona)
    Entonces
        Si (cualquiera de esos Grupos tiene No Access) Entonces
            El usuario tiene No Access
        Si no
            El usuario tiene los permisos acumulados de todos los grupos donde se lo menciona
Entonces
    Si (hay Listas de Usuarios donde se lo menciona)
    Entonces
        Si (cualquiera de esas listas tiene No Access)
        Entonces

El usuario tiene No access

Si no

El usuario tiene los permisos acumulados de todas las Listas de Usuarios donde se lo menciona

Si no

Si (Everyone está incluido en la lista)

Entonces

Si (Everyone tiene definido No Access)

Entonces

El usuario tiene No Access

Si no

El usuario tiene los permisos definidos para Everyone.

Si no

El usuario tiene No Access. (porque no está incluido en ninguna parte)

Tener en cuenta, que cada vez que aparece la expresión “Si no” en la lógica, se detiene el proceso de permisos de accesos si la condición anterior es verdadera. Esto es lo que define el orden de prioridad en la seguridad de ProjectWise. También, si se define Seguridad de Flujo de Trabajo y los permisos de usuario en la Seguridad de Objeto no están definidos como “No Access”, entonces prevalecerá la Seguridad de Flujo de Trabajo y **la misma lógica mostrada arriba para Seguridad de Objeto será ejecutada en el contexto de Seguridad de Flujo de Trabajo.** Los permisos definidos al nivel de Etapa prevalecerán sobres los permisos definidos al nivel de Flujo de Trabajo. Asimismo, los permisos de Flujo de Trabajo definidos específicamente para una carpeta prevalecerán sobre la herencia de Seguridad de Flujo de Trabajo de cualquier otra carpeta en el DataSource.

Recordar estas reglas cuando se determinen los derechos de acceso de los usuarios a los documentos:

- Apagar el Ajuste de Usuario “Use Access Control” hace de ese individuo un “súper usuario” que es inmune a los permisos de acceso definidos en ProjectWise.
- Ni la Seguridad de Objeto ni la de Flujo de Trabajo puede otorgar permisos (a un usuario) que no estén prendidos en Ajustes de Usuario (para dicho usuario).

Ajustes.

- Dentro de la estructura de carpetas, **Seguridad de Objeto** deberá ser lo primero a probar para ver si al usuario se le denegó acceso a través del ajuste “No Access”.
- Si a un usuario no se le niega explícitamente el acceso a través del ajuste “No Access” y se aplica **Seguridad de Flujo de Trabajo,** entonces el usuario tendrá todo permiso que se haya definido en los permisos de flujo de trabajo. Y si el usuario no está listado en los permisos de Flujo de Trabajo, entonces dicho usuario tendrá “No Access”.
- Las definiciones de Seguridad toman la siguiente prioridad de más alta a más baja: Usuario, Grupos, Listas de Usuario, Everyone

4.3 Autenticación y Encriptado

En la sección 4.0 se habló de la autorización sobre los objetos. Esto se logra utilizando Control de Acceso en varios métodos. Esto asume que el usuario ha sido autenticado en el sistema. Confidencialidad es el término utilizado para prevenir la divulgación de información a individuos o sistemas no autorizados. Permitiendo a ProjectWise administrar los datos y teniendo flujos de trabajo que permiten funcionalidad dentro de los environments, al mismo tiempo se asegura la seguridad de los datos. Se hace esto para mantener la integridad de los datos con conceptos de seguridad en el lugar, trabajando dentro de la infraestructura de la red. La aplicación tiene procesos en el lugar para asegurar la integridad de la seguridad al nivel de aplicación del sistema.

Cuando se habla de utilizar Autenticación y Encriptado debemos definir estos términos. Autenticación es el acto de establecer o confirmar que algo como un recurso, proceso o persona es *auténtico* , esto es que las demandas realizadas por o acerca del sujeto son verdaderas.

La identidad de un usuario de ProjectWise se debe verificar durante el **proceso de autenticación.** La Autenticación en ProjectWise involucra un proceso de dos pasos: ingresar información pública (username), y luego ingresar información privada (password). Cuando vemos la información pública es en realidad el paso de identificación, mientras que el ingreso de información privada es el paso de autenticación. En ProjectWise hay algunas opciones que agilizan este proceso si se está utilizando Active Directory. Se puede habilitar Single Sign On (SSO). Esto se puede usar cuando se utilice ProjectWise Synchronization Service para tomar las cuentas de dominio desde el Active Directory y poblarlas en ProjectWise. Una vez que el usuario de dominio está en ProjectWise se puede

Copyright © 2010 Bentley Systems, Incorporated

autenticar basado en el username y password que se le asignó en el computador local. ProjectWise Explorer pasa el username y password al ProjectWise Integration quien a su vez llama al controlador de dominio para asegurar que el username y password son válidos, de ahí ingresa a ProjectWise sin necesidad de ingresar username y password. Esta es una opción que se puede definir del lado del servidor en el archivo dmskrnl.cfg.

Ciertas políticas o standards pueden requerir que se aplique **fuerte autenticación** que contiene dos métodos. Esto también se refiere como **autenticación de dos-factores.** Para poder realizar este método es algo que una persona sabe, tiene o es. Esto puede ser como que alguien tiene una tarjeta CaC (Common Access Card) y algo que el usuario sabe como su password. Está bien utilizar estos dispositivos para autenticarse al sistema de operaciones local cuando se utiliza con ProjectWise, porque una vez logueado en el sistema operativo local se puede tener SSO habilitado y pasará las credenciales del usuario al ProjectWise Explorer y al ProjectWise Web Client.

Ahora que hemos hablado sobre autenticación, necesitamos ver **encriptado.** Este es el proceso de transformar información en formato texto común utilizando un algoritmo o cifrado que lo hace ilegible para todos excepto aquellos que posean conocimientos especiales, generalmente referido como llave. El resultado del proceso es información **encriptada** dentro de ProjectWise cuando se transfiere por el cable. Para realizar esto se debe ejecutar ProjectWise en modo seguro lo cual se discutirá mas adelante en sección 4.4.

Cuando se habla acerca de procesos de **Autenticación** y **Encriptado** lo hacemos para asegurar un par de cosas en cuanto a administración de datos y teniendo en cuenta conceptos de seguridad. **Confidencialidad** cuando se busca confidencialidad es para prevenir la divulgación no autorizada, intencional o no intencional, del contenido de ProjectWise, asegurando los archivos y ejecutables que utiliza ProjectWise. Aseguramos esto definiendo controles de acceso dentro de ProjectWise que permitir el acceso de ciertos usuarios y grupos de usuarios a ciertas carpetas y documentos como se vio en la sección anterior. **Integridad** asegura que los datos no podrán ser modificados por usuarios no autorizados dentro de ProjectWise. También aseguramos que no se realicen modificaciones no-autorizadas por usuarios autorizados. Dentro de ProjectWise se asegura esto definiendo el acceso correcto a ciertos usuarios o grupos al contenido que necesitan. Por ejemplo, dando permisos de sólo-lectura a ciertos usuarios y de escritura a otros dependiendo en la etapa del flujo de trabajo. **Disponibilidad** asegura el acceso a los datos y los recursos en tiempo y con seguridad dentro de ProjectWise. Dentro de ProjectWise dando permisos de acceso a los usuarios para que puedan realizar sus tareas. Sin restringir tanto que no puedan acceder al sistema. Servidores cluster y recupero por falla para asegurar un tiempo de recuperación optimo.

Preguntas Frecuentes sobre Autenticación y Encriptado de ProjectWise

¿Qué tipo de encriptado se utiliza cuando un usuario se loguea a la interface Web sin utilizar SSL?

Utiliza codificación estándar base64. El nombre del usuario se pasa como texto normal. Base64. Típicamente ser refiere a Base64 como un esquema de codificación y no encriptado. Es una codificación trivial y no se considera seguro.

¿Qué tipo de encriptado se utiliza cuando un usuario se loguea a la interface Web utilizando SSL?

Utiliza encriptado de 128 bit para el username y passwords que se pasan por el cable. La fortaleza de la sesión SSL entre el navegador y el servidor dependen en la fortaleza de la llave de sesión que se genera durante la negociación de la sesión. Esta es una llave simétrica que se utiliza para encriptar y desencriptar los datos intercambiados entre el navegador y el servidor. Los navegadores y los servidores generalmente negocian la mas fuerte sesión soportada mutuamente. Esto quiere decir que si el navegador del usuario y la Web soportan sesiones SSL de 12-bit, se establecerá una sesión de 128-bit. Si el navegador sólo soporta

Copyright © 2010 Bentley Systems, Incorporated

sesiones SSL de 40-bit, se establecerá una sesión de 40-bit, inclusive si el servidor Web soporta sesiones de 128-bit.

¿Qué tipo de encriptado se utiliza cuando un usuario se loguea a un datasource en ProjectWise Explorer utilizando una cuenta de dominio de Windows?

Utiliza método de autenticación y encriptado NTLM. También soporta autenticación Kerberos, pero ni NTLM ni Kerberos se utilizan para encriptado. Sin la activación por separado del encriptado SSL (entre el cliente y el servidor), sólo algunas partes mas sensitivas de algunos mensajes se encriptan por el algoritmo RC4 (utilizando llaves de 128 bit). Esto se realiza independientemente del protocolo de autenticación.

¿Qué tipo de encriptado se utiliza cuando un usuario se loguea a un datasource de ProjectWise Explorer utilizando una cuenta lógica de ProjectWise?

Utiliza el algoritmo RC4 de encriptado (utilizando llaves de 128 bit).

¿Qué tipo de encriptado se utiliza cuando un usuario se logue utilizando SSL en el ProjectWise Application Server donde están publicados los datasources (Ejecutando ProjectWise en modo seguro) ?

Utiliza encriptado de 128 bit del servidor de certificados en la red. Las llaves son validadas por el servidor que ejecuta el servidor de certificados. Sigue utilizando el puerto 5800. Me referiré a esto como "Conexión Segura de ProjectWise" cuando no se esté hablando de la interface Web utilizando HTTPS. SSL es un standard muy conocido y nuestra conexión no está basada en el mismo.

¿Puedo habilitar SSL con ProjectWise Explorer? ¿Se debe modificar la configuración de los puertos?

Utilizando ProjectWise en modo seguro encripta los datos desde el ProjectWise Explorer al servidor de aplicaciones. La configuración se realiza en el servidor. Las llaves de encriptado son manejadas por el servidor de certificados.

¿Se encripta el archivo cuando se transfiere por el cable utilizando ProjectWise?

Sólo cuando se utiliza ProjectWise con conexión segura.

¿Qué tipo de comunicación segura se realiza cuando se comunica con la base de datos?

ProjectWise se comunica con la base de datos a través de ODBC. ProjectWise utilizará el tipo de conexión que se haya configurado, no importa cuál sea. Por ejemplo, MS SQL Server pasando el username y password como texto simple. Se puede utilizar el Server Network Utility para habilitar el encriptado SSL sobre todas las librería de red habilitadas. SQL Server 2000 puede utilizar SSL para encriptar todos los datos que se transmiten por **cualquier** librería de red entre un cliente SQL Server 2000 (ProjectWise Application Server) y un servidor corriendo SQL Server 2000. El nivel de encriptado, 40-bit versus 128-bit, depende en el nivel de encriptado soportados por el sistema operativo Windows involucrado. depends on the level of encryption supported by the Windows operating system involved as well. Para una máxima seguridad se recomienda utilizar Microsoft integrated authentication para la conexión a las bases de datos.

¿Cómo trabaja ProjectWise con Active Directory?

ProjectWise trabaja con un modelo de Active Directory en modos Mixto y Nativo. ProjectWise Authentication Server tomará la información de usuarios y grupos de un AD, del controlador de Dominio.

Copyright © 2010 Bentley Systems, Incorporated

Una vez en ProjectWise los usuarios se autentican desde el servidor de aplicaciones de ProjectWise al controlador de Dominio en AD.

¿ProjectWise guarda mis Passwords en la Base de Datos?

Para los usuarios Windows de ProjectWise NO se guardan las passwords en la base de datos. El ProjectWise Authentication Server trae los nombres de usuarios del dominio dentro de la base de datos donde se guardan en la tabla DS_SID. Luego puebla los nombres de usuarios en la tabla dms_user. Cuando el usuario se autentica en ProjectWise, ProjectWise Application llama al controlador de dominio en tiempo real para autenticar al usuario. Por esta razón no se guardan las cuentas Windows de ProjectWise en la base de datos. Las passwords no se guardan en la base de datos. Sólo en los usuarios lógicos de ProjectWise, se guarda MD5 hash de las password para que estas no se puedan recuperar.

¿ProjectWise soporta Kerberos?

No directamente, ProjectWise trabajará con un Active Directory de Win2003 utilizando Kerberos. Autenticación utilizando Kerberos es soportada.

¿Si un usuario se loguea desde el cliente Web utilizando su cuenta NT, cómo se encarga ProjectWise de la password enviada por el cable? ¿Qué protocolo se utiliza?

Si no se utiliza SSL, ProjectWise usa una codificación Base64 y la password se codifica utilizando eso. Para un método mas seguro se recomienda utiliza SSL dentro del entorno Web.

¿Si un usuario se logue desde el cliente Web utilizando su cuenta de Windows/Single Sign On, cómo se encarga ProjectWise de la password enviada por el cable? ¿Qué protocolo utiliza?

Cuando se utilice el cliente Web utilizará protocolo http o https. Para asegurar encriptado, se recomienda utilizar https con un certificado de seguridad. En este tipo de configuración, toda la información transferida desde el cliente al servidor estará encriptada.

4.4 ProjectWise desde Afuera

Términos Utilizados

Resumen de ProjectWise trabajando dentro de la red. Listado de los diferentes puertos y avenidas de comunicación. Hablaremos de optimizar en forma segura a ProjectWise dentro de la infraestructura, analizando el proceso de trabajar en medio del “sistema” como un todo.

Los términos que referiremos son **Private LAN (Intranet)-** Una red que interconecta dispositivo en una misma oficina, piso o edificio. ProjectWise Application Server y ProjectWise Explorer residirán aquí. **DMZ (Extranet)-** Siglas para Demilitarized Zone, una computadora o una pequeña red que está entre una red interna confiable (LAN) y una red externa no confiable, como puede ser internet público. ProjectWise Web Server y ProjectWise Connection Server se pueden encontrar aquí.. **Secure Sockets Layer (SSL)-** SSL trabaja utilizando una llave privada para encriptar los datos que se transfieren por una conexión SSL. Protocolo utilizado para obtener información confidencial del usuario, como nombre de usuario y password. Por convención, las URLs que requieren una conexión SSL comienzan con https en lugar de http.

Copyright © 2010 Bentley Systems, Incorporated

Configurando el Setup

ProjectWise se puede implementar en muchas formas.. Puede ser interno a la compañía (LAN) y aplicar los permisos correctos basados en grupos dentro del dominio. Toda la comunicación es interna y no se necesita nada externo. También se puede implementar para trabajar con usuarios externos al dominio entonces se debe configurar el acceso externo (Extranet). Para poder hacer esto se deben tener algunas cosas en consideración. Se estará trabajando con usuarios de otras compañías, clientes o usuarios de la compañía pero que son externos. Lo mejor será crear grupos en el Active Directory para cada uno de estos usuarios y sincronizarlo con ProjectWise. Si no es posible, entonces se deben crear usuarios y grupos lógicos dentro de ProjectWise.

Trabajando en la Extranet

Una vez que se tiene ProjectWise instalado y corriendo internamente y se desee tener acceso desde afuera, se deberá configurar la infraestructura de red para que lo soporte. La mejor manera es aprovechar la Extranet de la compañía. Aquí se puede colocar el ProjectWise Gateway Server en DMZ y ProjectWise Web Server para acceso externo. El ProjectWise Gateway actuará como proxy para permitir a los usuarios acceder al ProjectWise Integration Server. El ProjectWise Gateway pasa información del cliente externo al Gateway Server y al ProjectWise Integration Server. El ProjectWise Gateway Server está en el DMZ y debería tener una IP pública junto con un Fully Qualified Domain Name (FQDN). Se recomienda utilizar FQDN incluso cuando es posible utilizar el IP externo. La razón por la cual se recomienda utilizar FQDN es porque es un DNS estático, con la adopción de direcciones IP IPV6 , no es fácil recordar el IP.

e.g. `2001:db8:85a3::8a2e:370:733.`

Una vez que ProjectWise Gateway Server Service y Web Server estén instalados en máquinas en el DMZ se debe realizar la conexión hasta el ProjectWise Integration Server Service. Si hay firewall entre los servidores, se deberá abrir el puerto bi-direccional 5800 entre los servidores. Para abrir el ProjectWise Explorer se deberá abrir el puerto 5800 bi-direccional externamente. Ahora los clientes externos sólo podrán ver el ProjectWise Gateway Server en el DMZ. ProjectWise Web Server utiliza los puertos 80 si se utiliza http o 443 si se utiliza SSL. Se recomienda utilizar SSL y el puerto 443.

El cliente se conectará al ProjectWise Gateway Server Service utilizando el FQDN en Network Control Utility en ProjectWise Explorer. Se pueden ejecutar, tanto ProjectWise Explorer como ProjectWise Web para que usen SSL. Si se define esto para ProjectWise Explorer se debe ejecutar ProjectWise en “Secure mode” y si se utiliza ProjectWise Web Server configurar IIS para que utilice una conexión segura para toda llamada realizada utilizando el protocolo https para tráfico web. La comunicación punto-a-punto se encripta cuando se ejecuta ProjectWise en modo-seguro.

Copyright © 2010 Bentley Systems, Incorporated

4.5 TBD

TBD

4.6 TBD

TBD

Copyright © 2010 Bentley Systems, Incorporated

5.0 Materiales Relacionados y de Referencia

DRAFT

Copyright © 2010 Bentley Systems, Incorporated